WIRELESS FINGERPRINT BASED STUDENT ATTENDANCE SYSTEM

A thesis submitted in partial fulfillment of
the requirements for the degree of
Bachelor of Technology
in
Electrical Engineering

by

Debidutt Acharya(10602015)
and
Arun Kumar Mishra(10602061)

Under the guidance of

Prof. Susmita Das

Department of Electrical Engineering
National Institute of Technology
Rourkela-769008

2010

WIRELESS FINGERPRINT BASED STUDENT ATTENDANCE SYSTEM

A thesis submitted in partial fulfillment of
the requirements for the degree of
Bachelor of Technology
in
Electrical Engineering

by

Debidutt Acharya(10602015)

and

Arun Kumar Mishra(10602061)

Department of Electrical Engineering

National Institute of Technology

Rourkela-769008

2010

National Institute of Technology

Rourkela

CERTIFICATE

This is to certify that the thesis entitled, "WIRELESS FINGERPRINT-BASED STUDENT ATTENDANCE SYSTEM" submitted by Debidutt Acharya and Arun Kumar Mishra in partial fulfilments for the requirements for the award of Bachelor of Technology Degree in Electrical Engineering at National Institute of Technology, Rourkela is an authentic work carried out by them under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University / Institute for the award of any Degree or Diploma.

Date: 14-05-2010

Place: Rourkela

Prof. Susmita Das
Deptt. of Electrical Engineering
National Institute of Technology
Rourkela

ACKNOWLEDGEMENT

I would like to express my deepest sense of gratitude towards my supervisor, Prof. Susmita Das who has given me much suggestion, guidance and support.

I would like to thank all the staff members of Department of Electrical Engineering for their extended cooperation and guidance.I also take this opportunity to give thanks to all others who have given me support for the project or in other aspects of my study at National Institute of Technology.

Debidutt Acharya
10602015

Arun Kumar Mishra
10602061

Date: 14-05-2010
Place: Rourkela

WIRELESS FINGERPRINT BASED STUDENT ATTENDANCE SYSTEM

Abstract

Our B. Tech. Project aims at introducing biometric capable technology for use in automating the entire attendance system for the students pursuing courses at an educational institute. The goal can be disintegrated into finer sub-targets; fingerprint capture & transfer, fingerprint image processing and wireless transfer of data in a server-client system. For each sub-task, various methods from literature are analyzed. From the study of the entire process, an integrated approach is proposed.

Biometrics based technologies are supposed to be very efficient personal identifiers as they can keep track of characteristics believed to be unique to each person. Among these technologies, Fingerprint recognition is universally applied. It extracts minutia- based features from scanned images of fingerprints made by the different ridges on the fingertips. The student attendance system is very relevant in an institute like ours since it aims at eliminating all the hassles of roll calling and malpractice and promises a full-proof as well as reliable technique of keeping records of student's attendance.

CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

1. INTRODUCTION

1.1Introduction

The human body has the privilege of having features that are unique and exclusive to each individual. This exclusivity and unique characteristic has led to the field of biometrics and its application in ensuring security in various fields. Biometrics has gained popularity and has proved itself to be a reliable mode of ensuring privacy, maintaining security and identifying individuals. It has wide acceptance throughout the globe and now is being used at places like airports, hospitals, schools, colleges, corporate offices etc.

Biometrics is the very study of identifying a person by his/her physical traits that are inherent and unique to only the person concerned. Biometric measurement and assessment include fingerprint verification, iris recognition, palm geometry, face recognition etc. The above mentioned techniques work with different levels of functionality and accuracy.

Accuracy and reliability are the two most important parameters when it comes to biometric applications. Fingerprint verification is one of the oldest known biometric techniques known but still is the most widely used because of its simplicity and good levels of accuracy. It’s a well known fact that every human being is born with a different pattern on the fingers and this feature is exploited to identify and differentiate between two different persons.

The application in an educational institute is worth noting because of the benefits it brings along with it. The fingerprint recognition and verification technique can easily replace an attendance sheet and save time wasted on calling out roll numbers in the class. A fingerprint detecting device needs to be placed in each classroom and students would be made to swipe their finger over the sensor so as to mark their presence in the class. The database would contain all the fingerprints beforehand. So, the moment a finger would be swiped, a check would be carried out

with the existing database and the corresponding student would get a present mark on his attendance record maintained in a server.

The transfer of the fingerprint from the device to the server can be carried out wirelessly using certain wireless adapters which can together form a wireless network in a short range and carry out the verification process. The communication channel needs to be secured and should be kept free from interference as far as possible. For further security of the entire system and to detect illegal activities, a security camera can be installed to keep track of the enrollments made in the classroom.

Chapter 2

Fingerprint

2. FINGERPRINT

2.1 What is a fingerprint?

A fingerprint, as the name suggests is the print or the impression made by our finger because of the patterns formed on the skin of our palms and fingers since birth. With age, these marks get prominent but the pattern and the structures present in those fine lines do not undergo any change. For their permanence and unique nature, they have been used since long in criminal and forensic cases.

Shown below, is a fingerprint pattern obtained from an optical sensor. The figure shows faint and dark lines emerging from a particular point and spiraling around it all over the finger.

Figure 2.1.1 A fingerprint image acquired by an optical sensor

Every fingerprint consists of ridges and furrows. These ridges and furrows are known to show good similarities but when it comes to identifying a person or distinguishing between two different prints, these do not prove efficient enough. Research shows that fingerprints are not distinguished by ridges and furrows but by Minutia. Minutia refers to some abnormalities in a ridge, which shall be discussed in detail in the following pages.

As already mentioned, Minutia are abnormal points in a ridge. There can be various such Minutia but the two most important and useful minutia types are Termination and Bifurcation. Termination refers to the abrupt ending of a ridge, as shown in fig.2.2.1. Bifurcation on the other hand refers to the point on the ridge where branching occurs, as shown in fig.2.2.2

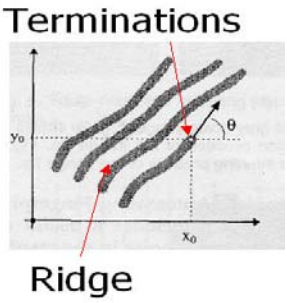


Figure 2.1.2 Termination minutia

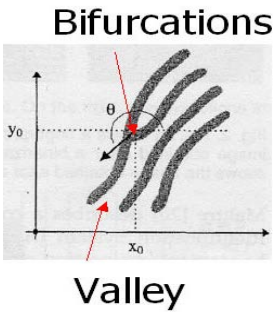


Figure 2.1.3 Bifurcation minutia(Furrow, also known as valley

2.2 Fingerprint Recognition

Once the fingerprint is captured, the next step is the recognition procedure. The recognition procedure can be broadly sub grouped into

a. Fingerprint identification
b. Fingerprint verification

Fingerprint identification refers to specifying one's identity based on his fingerprints. The fingerprints are captured without any information about the identity of the person. It is then matched across a database containing numerous fingerprints. The identity is only retrieved when a match is found with one existing in the database. So, this is a case of one-to-n matching where one capture is compared to several others. This is widely used for criminal cases.

Fingerprint verification is different from identification in a way that the person's identity is stored along with the fingerprint in a database. On enrolling the fingerprint, the real time capture will retrieve back the identity of the person. This is however a one-to-one matching. This is used in offices like passport offices etc. where the identity of a person has to be checked with the one provided at a previous stage.

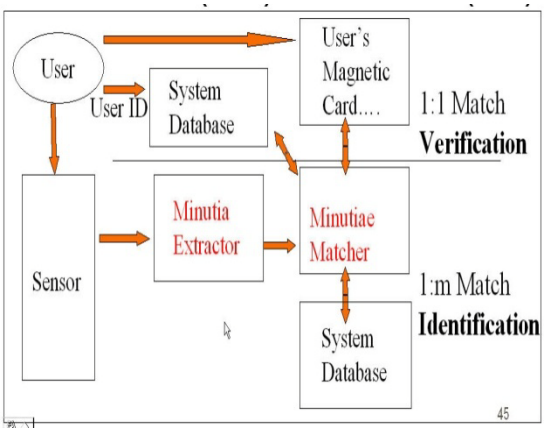


Fig 2.2.1: Verification Vs Identification

Irrespective of the procedure carried out, the fingerprint recognition has to be such that the fingerprint is well- represented and retains its uniqueness during the process. In the following pages, an approach to fingerprint recognition has been discussed that will deal with the representation of the same.

2.3 Approach to fingerprint recognition

The approach that we have concentrated on in recognition of the fingerprints is the minutia based approach. In this approach the ridge bifurcations and terminations are taken into consideration for analyzing each fingerprint. The representation is based on these local features.

The scanner system uses highly complex algorithms to recognize and analyze the minutia. The basic idea is to measure the relative portion of minutia. Simply, it can be thought of as considering the various shapes formed by the minutia when straight lines are drawn between them or when the entire image is divided into matrix of square sized cells. If two fingerprints have the same set of ridge endings and bifurcations forming the same shape with the same dimension, there' s a huge likelihood that they are of the same fingerprint.

So, to find a match the scanner system has to find a sufficient number of minutia patterns that the two prints have in common, the exact number being decided by the scanner programming.

Chapter 3

Fingerprint Image Processing

3. FINGERPRINT IMAGE PROCESSING

The fingerprint image is processed through a three step procedure. The image undergoes pre-processing, minutia extraction and post-processing. The three stages involve different steps and procedures which need to be discussed in detail.

3.1 Pre-processing

The pre-processing stage makes use of image enhancement, image binarization and image segmentation.

3.1.1 Image Enhancement

Image enhancement is necessary to make the image clearer for further operations. The fingerprint images obtained from sensors are not likely to be of perfect quality. Hence, enhancement methods are used for making the contrast between ridges and furrows higher and for maintaining continuity among the false broken points of ridges, which prove to ensure a higher accuracy for recognition of fingerprint.

Generally two types of procedures are adopted for image enhancement:

1) Histogram Equalization; 2) Fourier Transform.

3.1.1.1 Histogram Equalization

Histogram equalization is responsible for expanding the pixel distribution of an image in order to increase perceptional improvement. The pictorial description is given below. The fingerprint initially has a bimodal type histogram as shown in fig 3.1. After histogram equalization is carried out, the image occupies the entire range from zero to 255, enhancing the visualization effect in the process.

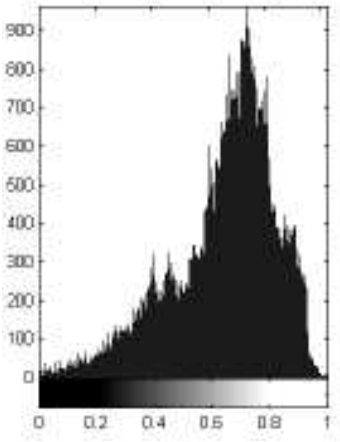


Figure 3.1.1.1 Fingerprint with original histogram (source : ref [13])

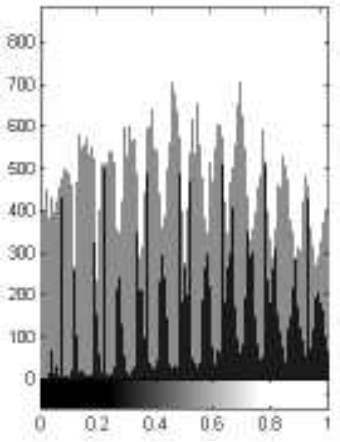


Figure 3.1.1.2 After histogram equalization (source: ref [13])

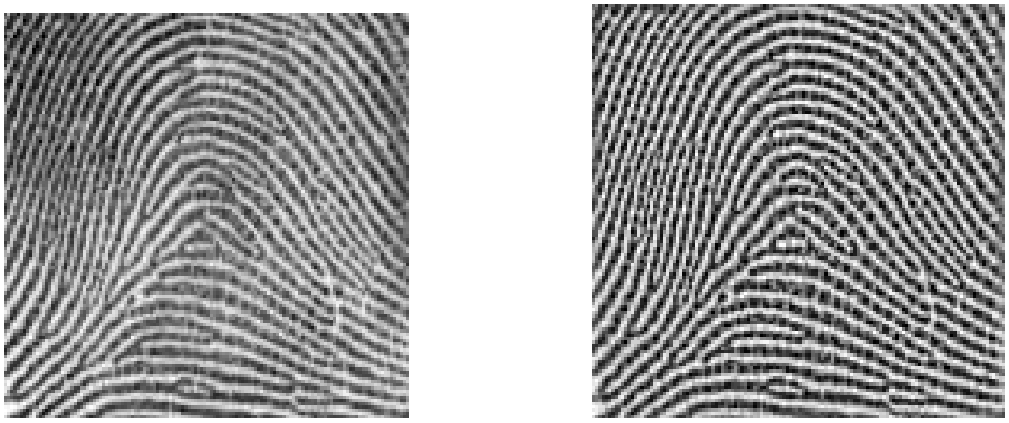


Figure 3.1.1.3 Effect of Histogram equalization(Source: ref [13])
Original Image Enhanced Image

3.1.1.2 Using Fourier Transform

In this process of enhancement the image is divided into small processing blocks (32 x 32 pixels) and Fourier transform is performed.

The function is as follows:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

For u= 0,1,2, … ,31

v= 0,1,2, ….,31

For enhancing a particular block by its dominant frequencies, the FFT os the block is multiplied by its magnitude a few times. Where the magnitude of the FFT is given by abs F(u,v) = |F(u,v)|.

The enhanced block can be obtained as per

$$g(x,y) = F^{-1}\left\{F(u,v) \times \left|F(u,v)\right|^{K}\right\} \quad (2)\ ,$$

where the inverse of (F(u,v)) is found by:

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times \exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \quad (3)$$

for x = 0, 1, 2, ..., 31 & y = 0, 1, 2, ..., 31 .

The k is a constant whose value has been experimentally found.Here,k is chosen as 0.45. When k is higher, the ridges appear improved, since the holes in the ridges are filled up, but at the same time a very high value results in false ridge joining.

Figure 3.1.1.4 depicts FFT enhanced image.

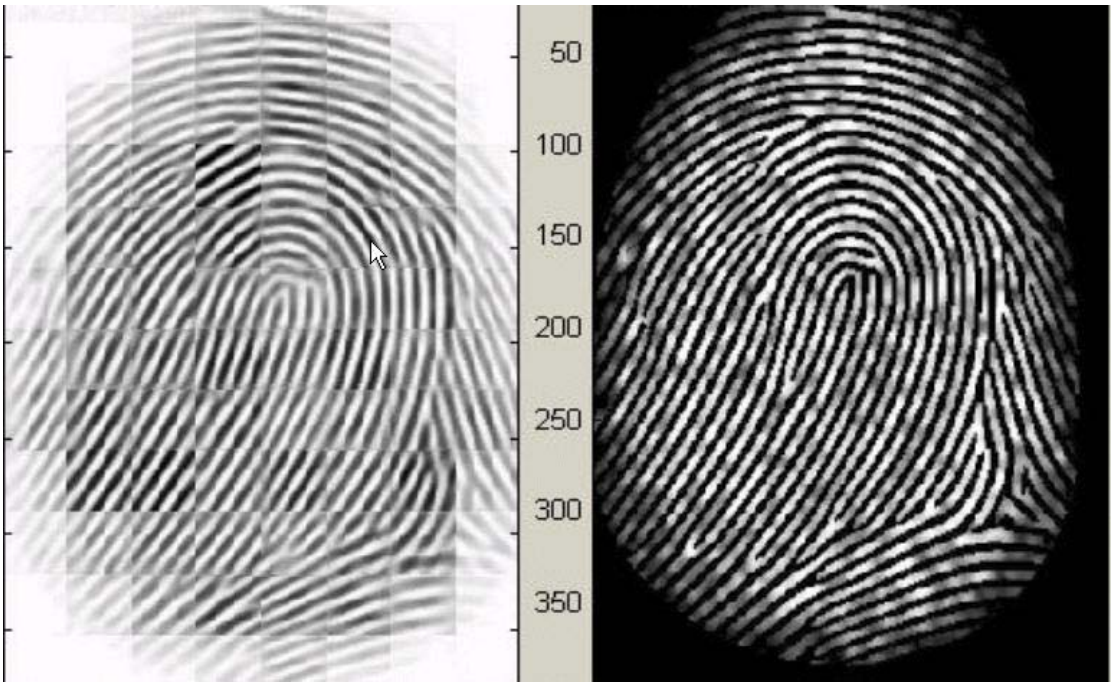


Figure 3.1.1.4 FFT enhanced fingerprint image(Source: Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, Handbook of Fingerprint recognition)

Before Enhancement After Enhancement

The image after enhancement connects falsely broken points on the ridges and removes spurious connections in between the ridges.

3.1.2 Image binarization

The original image is a 8-bit grayscale image. This process transforms the original image into a 1-bit image that assigns values 0 for ridges and 1 for furrows. After binarization, the ridges appear black while the furrows appear white.

Binarization changes the pixel value to 1 if the value is found to exceed the mean intensity of the current block to which it belongs.

The figure clearly depicts the effect of binarization on a normal grayscale image that has been only enhanced.

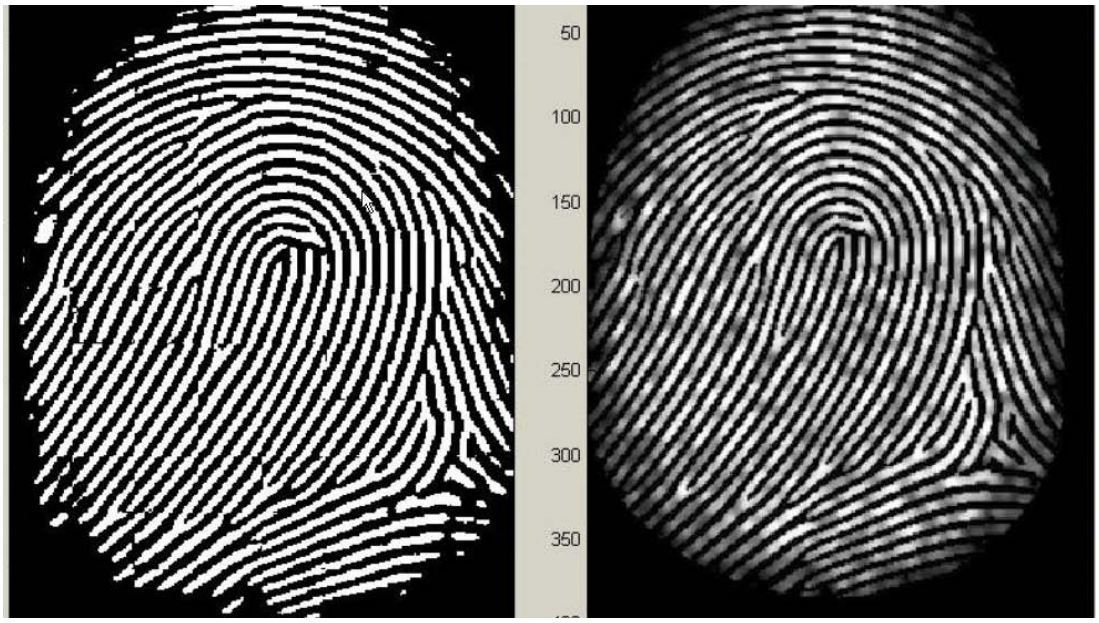


Figure 3.1.2 Effect of binarization

Binarized Image Gray image

3.1.3 Image segmentation

For a fingerprint image, only a certain portion is important which can provide the required information and can be useful for further processing. This portion is called the ROI or the region of interest. In this process, the area without important ridges and furrows is discarded as it holds only background information. After discarding those parts, the boundary of the remaining area is sketched out to get a clearer picture that is free from spurious minutia.

This process of segmentation is carried out in two steps. The first step is block direction estimation and the next ROI extraction by morphological methods. The details of the two steps are as follows.

3.1.3.1 Block direction estimation

The block direction for every block of the image is estimated. The algorithm is:

i. Calculation of gradient values for x-direction (p_x) and y-direction (p_y) for each pixel of the block using two Sober filters.

ii. Obtaining Least Square Approximation of block direction for each block using the following formula.

$$tp2ß = 2 \sum \sum (p_x * p_y) / \sum \sum (p_x^2 - p_y^2)$$

Considering the gradient values p_x and p_y as cosine value and sine value respectively, the tangent value of block direction can be estimated as given by the following formula:

$$tp2\theta = 2\sin\theta\cos\theta / (\cos^2\theta - \sin^2\theta)$$

The blocks with insignificant information are discarded as mentioned above using the following formula.

$$E = \{2 \sum \sum (p_x * p_y) + \sum \sum (p_x^2 - p_y^2)\} / W*W*\sum \sum (p_x^2 + p_y^2)$$

If certainty level E is found to be less than a threshold, then it is considered as a background block. A direction map is depicted in the figure below.

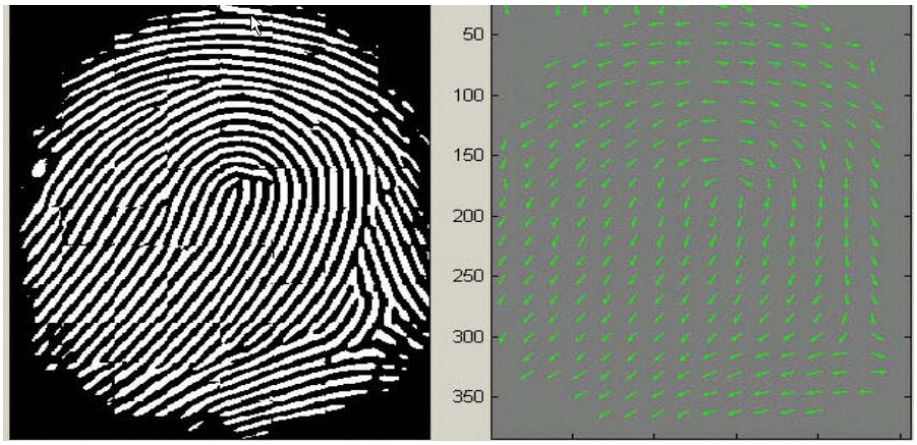


Figure 3.1.3.1 Effect of block direction estimation

Direction map (right)

3.1.3.2 ROI extraction by morphological methods

For carrying out morphological operations, two operations "OPEN" and "CLOSE" are defined. The OPEN operation (fig 3.1.3.3) has capability to inflict enhancement of an image and removal of peaks caused by noise while the CLOSE operation (fig3.1.3.2) is effective in shrinking images so as to remove small cavities.

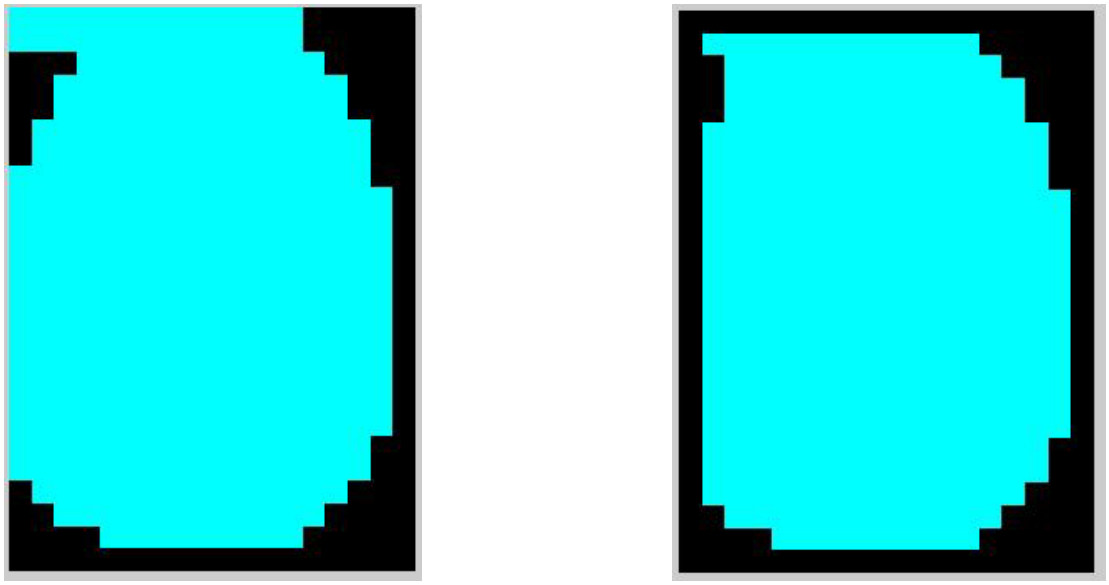
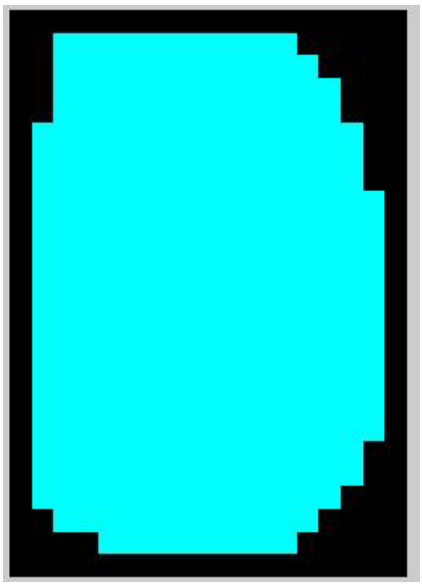


Figure 3.1.3.2 CLOSE operation

Before CLOSE operation After CLOSE operation



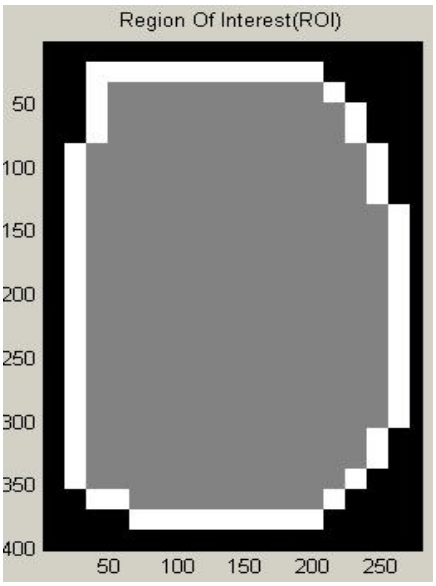


Figure 3.1.3.3 OPEN operation

After operation OPEN ROI + Bound

The bound is the remnant of the closed area out of the opened area. Then the algorithm throws away those extreme left, right, upper and bottom blocks out of the calculated bound so that we get the bounded region only containing the bound and inner area.

3.2 Minutia Extraction

The minutia extraction process involves ridge thinning followed by minutia marking

3.2.1 Ridge thinning

Ridge Thinning gets rid of repetitive pixels of ridges until the ridges are just one pixel wide. An iterative thinning algorithm is used. In every scan of the full image, the algorithm notes down repetitive pixels in each small image window. Finally all those marked pixels are removed after several scans. It can extract thinned ridges directly from gray-level fingerprint images. The method traces the ridges with highest gray intensity value. However, binarization is virtually enforced since the pixels with a high gray intensity value remain.

3.2.2 Minutia marking

This follows the ridge thinning process. The mechanism behind the minutia marking process is described as follows.

For every 3x3 window, if the pixel at the middle is one and has exactly three single-value neighbors, then the pixel is a ridge branch. If the pixel at the middle is 1 and has only one single-valued neighbor, then it means the central pixel is ridge ending.

The mean ridge width D is calculated at this point. The mean inter-ridge width is the mean distance between two nearby ridges. The method to approximate the D is easy. A row of the thinned ridge is scanned and the pixels with value one re summed up. Then the row length is divided with the summation above to get inter ridge width. For better reults, such row scans are performed several times and column scans too are conducted. Finally the mean of all the widths are calculated to get the D.

3.3 Post-processing

The final step is carried out to fine tune the image by processes like removing false minutia and unifying terminations and bifurcations.

3.3.1 False minutia removal

The preprocessing & minutia-extraction stage does not yield the final processed fingerprint image. False minutia such as false ridge breaks because of lack of ink and also ridge cross-connections from ink spill are still present. Also the earlier steps in processing themselves allow some errors. False minutiae can significantly affect accuracy of matching. So mechanisms to remove them are important.

False minutia can be of different types as follows

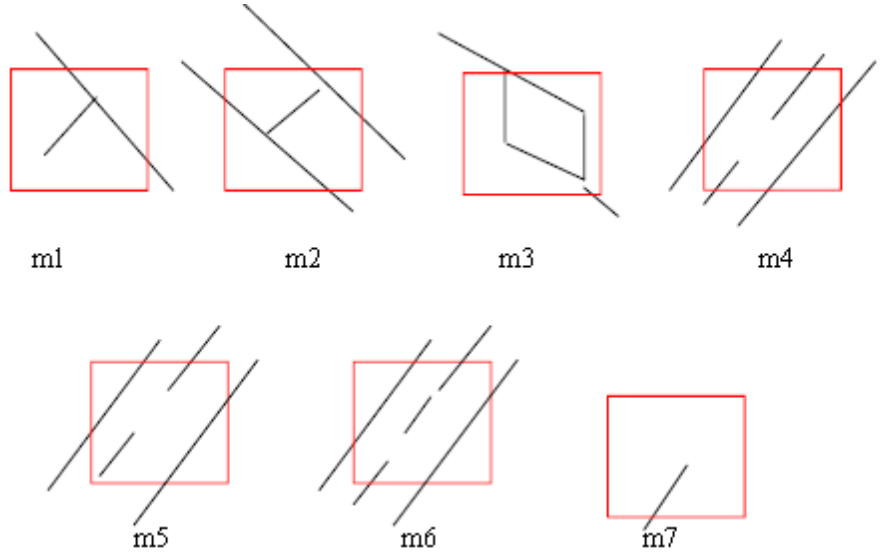


Figure 3.3.1 False minutia structures

m1 is case of a spike entering a ridge. In the m2, a spike connects falsely two valleys. m3 has two branching almost in the same ridge. Moving to m4, the two broken points on the ridge have almost the same orientation and also a short distance. m5 is alike the m4 case with the difference of one part being so short that another end is generated. m6 adds to the m4 case but with the extra condition that a third ridge is found at the centre of the parts of the broken ridge.

The procedure for removal of false minutia are as follows:

1. If the distance separating a bifurcation and termination is found to be less than D and two minutia belong to one ridge (m1) both of them are eliminated. Where D is the mean inter-ridge distance portraying the mean distance between two parallel nearby ridges.

2. If the width between two bifurcations is found less than D and they belong to one ridge, the two bifurcations are removed (m2, m3).

3. If two endings are within some predetermined distance D and their respective directions match with a small angle variation. And they support the condition that no any other ending is located between the two endings. Then the two terminations are considered to be false and is removed. (m4, m5, m6).

4. If two endings are located in a ridge with width less than D, the two are removed(m7).

3.3.2 Unification of terminations and bifurcations

Unification representation is used to avoid interference due to various data acquisition system conditions such as impression pressure. Mostly this representation is adopted for both termination and bifurcation. Hence, each individual minutia is characterized by the following parameters:

1) x-coordinate
2) y-coordinate
3) Orientation.

Chapter 4

System Design

4. SYSTEM DESIGN

The design of fingerprint based wireless attendance system can be divided into the four different modules. They are-

Processor Module

Fingerprint Capture Module

Wireless Module

PC based Server-Client Software Management Module

The module-wise approach to the design of the system helps in better understanding of the individual function levels. Also, a parallel approach to the system helps in distributing the effort on a multi-level range and helps in identifying the best features and available products in the market that suit the design requirements.

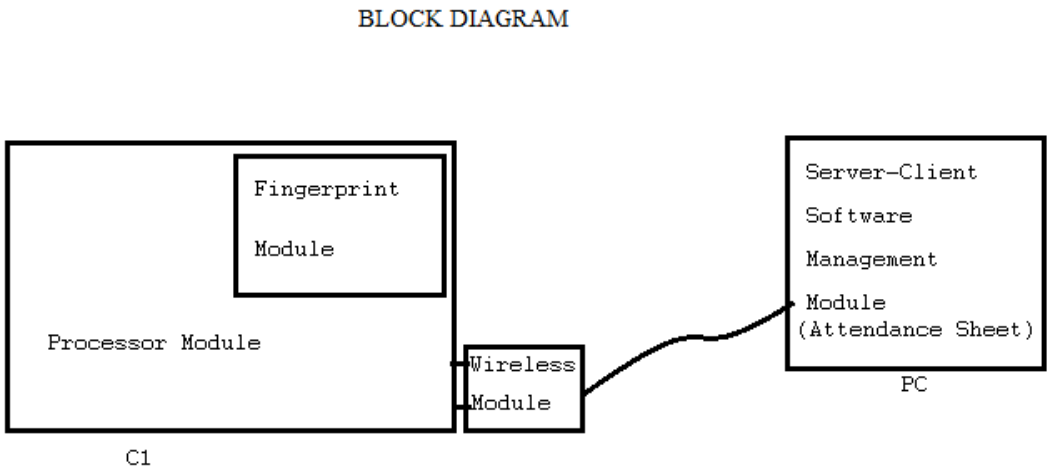


Fig. 4.1 Block Diagram showing the various modules in the System Design

4.1 Module Design

To view the system as an assemblage of four sub-components helps in simplifying the design problem. The three modules, i.e. Processor module, Fingerprint Capture module and Wireless module form the Client Hardware Module. The respective modules and their roles are explained below:

Processor Module: It forms the backbone of the system. It drives the control logic behind every functionality, some of which are mentioned below:

Power up and initialize itself and dependent modules.
Check for interrupts, faults while the modules get initialised.
Command the fingerprint module to function as requested by the software interface.
Enable data transfer through the wireless module.

Fig 4.1.1. A Digital Signal Processor (courtesy: www.rims.com.pk)

Fingerprint Capture Module(FCM): The fingerprint capture module is essentially a fingerprint sensor. It is an electronic device that captures a 'live scan' of the fingerprint pattern. Then a number of processing functions are applied to the scan and it is converted into a biometric template. Generally optical sensors are used, even though ultrasonic and capacitive sensors are also present.

Fig 4.1.2. A Fingerprint Sensor (courtesy: www.tradenote.net)

Wireless Communication Module(WCM): For the purpose of data transmission between various client modules (individual CHM setup in each classroom) and the server (PC) through a wireless channel, cost effective wireless module is used.

Fig 4.1.3. Rabbit Wireless Module (courtesy: www. embedded-system.net)

PC based Server-Client Software Management Module: The entire system is run from control software. The software on the server side consists of a database management and a GUI- based interactive Student Attendance System. The client side software is loaded into each CHM and governs the functioning of the CHM.

4.2 Algorithm Design

The software side of the design consists of implementing the following functions:

- Initialization of individual CHM
- Fingerprint Capture
- Wireless Data Transfer
- Fingerprint Image Processing
- Updating the database and attendance sheets
- Maintenance of GUI to Student Attendance System

Chapter 5

Wireless Data Transfer

5. WIRELESS DATA TRANSFER

After the fingerprint image has been processed, the data is to be transferred to the central server through a wireless channel. The data packet is to be coded into an encrypted form due to the sensitive nature of the information it carries. The data communicated to the server is broadly classified into two types:

- Enrol Data
- Daily Attendance Data

5.1 Enrol Data

This data is initially obtained when adding the new students to the institute database. Along with Personal Identification Numbers (PIN), student-specific data such as degree program, date of birth (DOB), student picture & signature, the database is provided with a biometric template consisting of a processed image of the fingerprint.

5.2 Daily Attendance Data

Once all the students are enrolled into the institute's Student Attendance System, the daily work of each CHM is to accumulate the attendance data for each course for a particular classroom and transmit the data to the Central Server System (CSS). This data can be of two types:

i. Choice 1: Only the Status of Presence (SoP) of each student in the particular classroom is combined with his/her respective PIN (say Roll Number) into a Student Presence Data Packet (SPDP). Each SPDP is aggregated for the entire batch of students for the classroom and a Final Data Packet (FDP) is formed.

This FDP is then transmitted to the CSS for each course class taken for that particular day.

ii. Choice 2: The entire Fingerprint Template (FT) of each student present in that particular course class who performs a successful fingerprint capture at the CHM is combined with his/her respective PIN (say Roll Number) to form a SPDP. The SPDP of students present is accumulated into a FDP and this FDP is then transmitted to the CSS for that particular course class.

To decide about the choice of FDP from the above two options, we must look into the various pros & cons associated with each of them. Below is presented a comparative study of the various factors related to the above two choices.

FACTORS	CHOICE 1	CHOICE 2
Programming Complexity	More	Less
Data Packet Complexity	Less	More
Processing Time	More	Less
Time to Wait*	More	More

*Time to Wait (ToW): Time to Wait is defined as the time required before the CHM becomes ready to accept the next input fingerprint image through the Fingerprint Capture Module (FCM).

Clearly, we can see that the choice 2 option seems more appropriate. Regarding the data packet complexity, it is safe to assume that wireless channel remains relatively idle for the major part of the time and hence data can be transmitted from each individual CHM to CSS immediately, or by CSS defined rule. Either a timing-based or a response-based rule may be used to accept data from each CHM.

On the CSS, the receiving wireless communication module (WCM) accepts the FDP from each CHM and converts it from electrical signals to digital data packets

(DDP) which are then sent to the Server. The Server then parses each DDP, decomposes it into individual SPDP and then each SPDP into respective PIN and attendance data** and determines the type of data the FDP contains; whether it carries an Enroll Data or Daily Attendance Data.

**The attendance data may be SoP for Choice 1 or FT for Choice 2.

If it finds that the received FDP contains Enroll Data, then it accesses the Fingerprint Database System, to add a new student to the institute database. If on the other hand it finds that the received FDP contains Daily Attendance Data, it may have to access both the Fingerprint Database and the Attendance Database. For the option of Choice 1, Attendance Database is updated directly with the latest attendance data using each individual SoP for that particular course class. For the option of Choice 2, the received FDP is decomposed into individual SPDP. Then each SPDP is decomposed into the respective PIN and its FT. First the Fingerprint Database is accessed using the respective PIN and then a Server-side matching of the two fingerprint templates is done. If match happens, the Attendance Database is updated. This step is performed for every DDP received.

Chapter 6

Experimental Setup

6. EXPERIMENTAL SETUP

The actual testing for the design of the wireless fingerprint based student attendance system was carried out in Communications Lab., Department of Electrical Engineering. The experimental setup consists of both software based platform and hardware module in an integrated development environment. The various components of the testing environment are:

- TMS320C6713 DSK
- AFS8500/8600 (Daughter Card)
- Wireless G Desktop Adapter
- Code Composer Studio v2.0
- FRT in MATLAB

The individual components are illustrated in the subsequent pages in detail.

6.1 TMS320C6713 DSK

This is a SPECTRUM DIGITAL product that includes a Texas Instrument's DSP TMS320C6713 operating at 225 MHz, mounted over a DSP Starter Kit complete with JTAG emulation through on-board JTAG emulator with USB host interface or external emulator and a host of other features.

Fig 6.1. TMS320C6713 DSK (courtesy: http://www.focus.ti.com)

The TMS320C6713 DSK functions as the Processor Module with the option of either simply controlling the Fingerprint Module or along with control of Fingerprint Module, also carrying out the fingerprint image processing and creation of the Fingerprint Template.

6.2 AFS8500/8600 Daughter Card

It is a Texas Instruments product provided with an optical sensor for fingerprint image capture.

Fig 6.2. FDC-AFS8600 Sensor Board Mounted on C6713 DSK (courtesy:)

It functions as the Fingerprint Capture Module.

6.3 Wireless G desktop adapter

Known by its product name DWA-510, the D-Link Wireless G DWA-510 Desktop adapter features the very latest in advanced wireless silicon chip technology to deliver a maximum wireless signal rate of up to 54Mbps* in the 2.4GHz frequency. Some of its features are:

• Faster Wireless Networking.

• Compatible with 802.11b and 802.11g Devices

• 32-bit PCI Performance/Plug & Play Connectivity

• User-friendly configuration and diagnostic utilities.

Fig 6.3. Wireless G DWA-510 Desktop Adapter (courtesy:)

This functions as the wireless communication module for the purpose of data transfer between two PC. Security features such as WPA, WPA2, and WEP allow for secure and encrypted channel.

6.4Code Composer Studio v2.0

Code Composer Studio (CCS) from Texas Instruments consists of a host of utilities that can be used for development and debugging of embedded applications. It provides a fast & comfortable interface to each step of code development. Special support for TI's devices such as compilers, source code editor, project build environment, debugger, profiler, simulators and many other features are included.

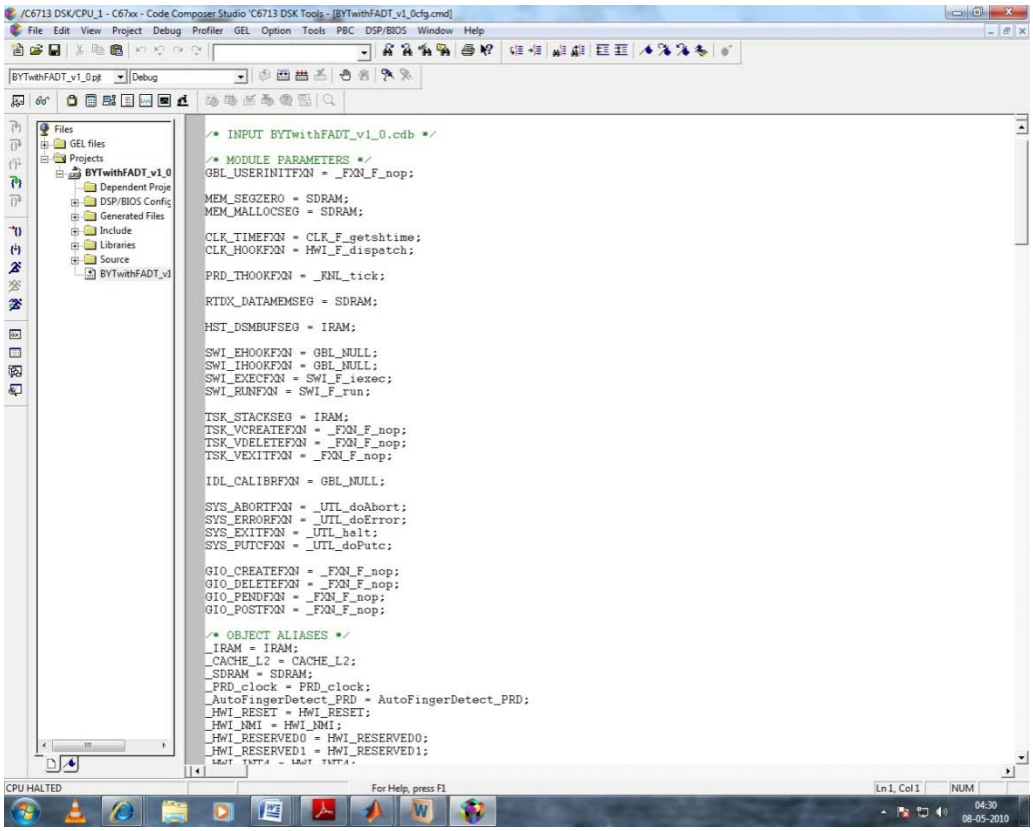


Fig 6.4. CCS IDE

6.5Fingerprint recognition toolbox

A new toolbox downloaded from the MATLAB CENTRAL website at www.mathworks.com allows us to add fingerprints to the database. Also it allows us to do a 1: n fingerprint match for verification.

It includes the various functions listed below:

- Fingerprint image visualization
- Gabor filter visualization
- Image enhancement
- Orientation field estimation
- Core point localization

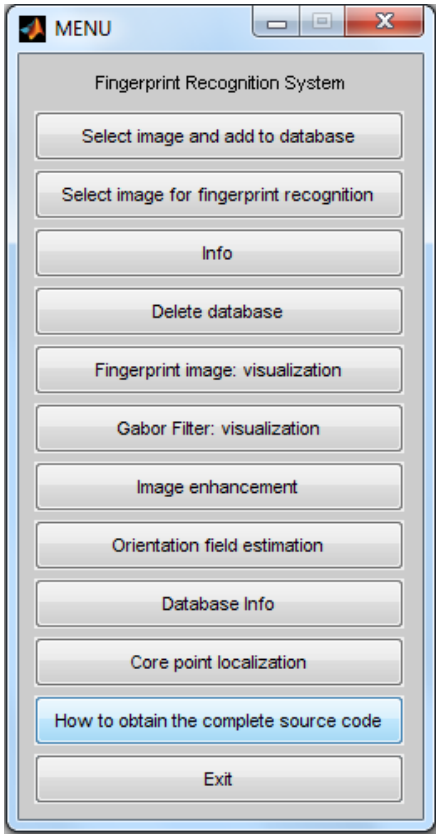


Fig 6.5 : FRT in MATLAB

Chapter 7

Result

7. RESULT

Initial progress is mentioned below:

i. The DSP starter kit TMS320C6713 and the Daughter card AFS8500/8600 were tested for proper functioning. The two were found to work properly.

ii. A demo software was run on the fingerprint module and its operation was analyzed. It was observed to be an Enroll-Once-Verify-Once software. The threshold for content matching was very low and flexibility for different orientations of the finger was not present.

iii. Established wireless network involving two terminals using DWA-510.

The main objective of the project then was to enroll fingerprints of different students and add them to the database which would be referred at the time of verification. For this purpose, Fingerprint Recognition Toolbox provided for use in MATLAB was used. For a particular trial run of the system, fingerprints of eight students were captured using the hardware kit in the lab and fingerprint image of seven were added to the database. The templates stored were named from s1 to s7. To show the successful functioning of the system three sample outputs are provided that show

i. Addition to database (result1)
ii. A fingerprint match for s1 (result2)
iii. A fingerprint match for s8 (result3)

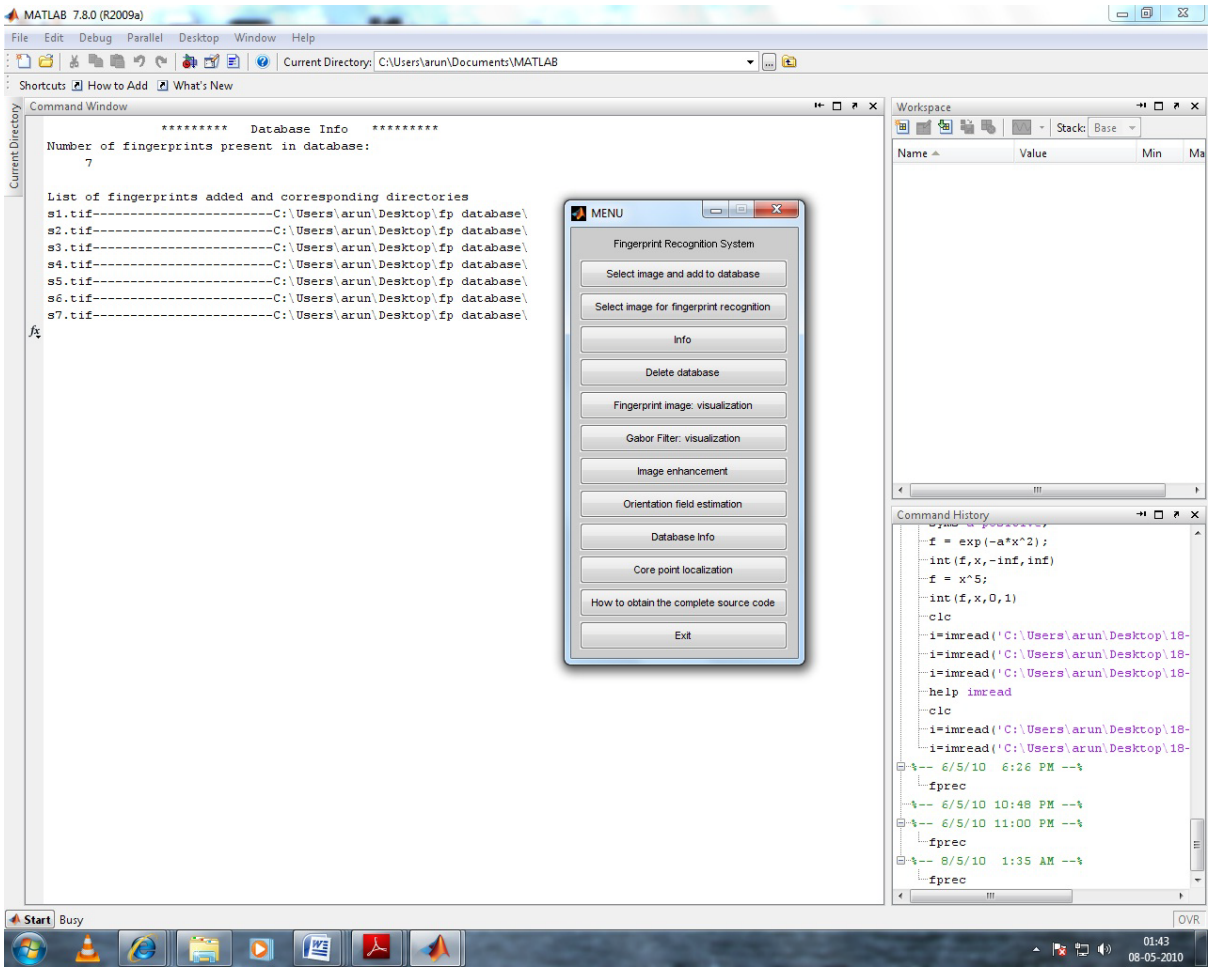


Fig 7.1.1 Sample Matlab Output (Result1)

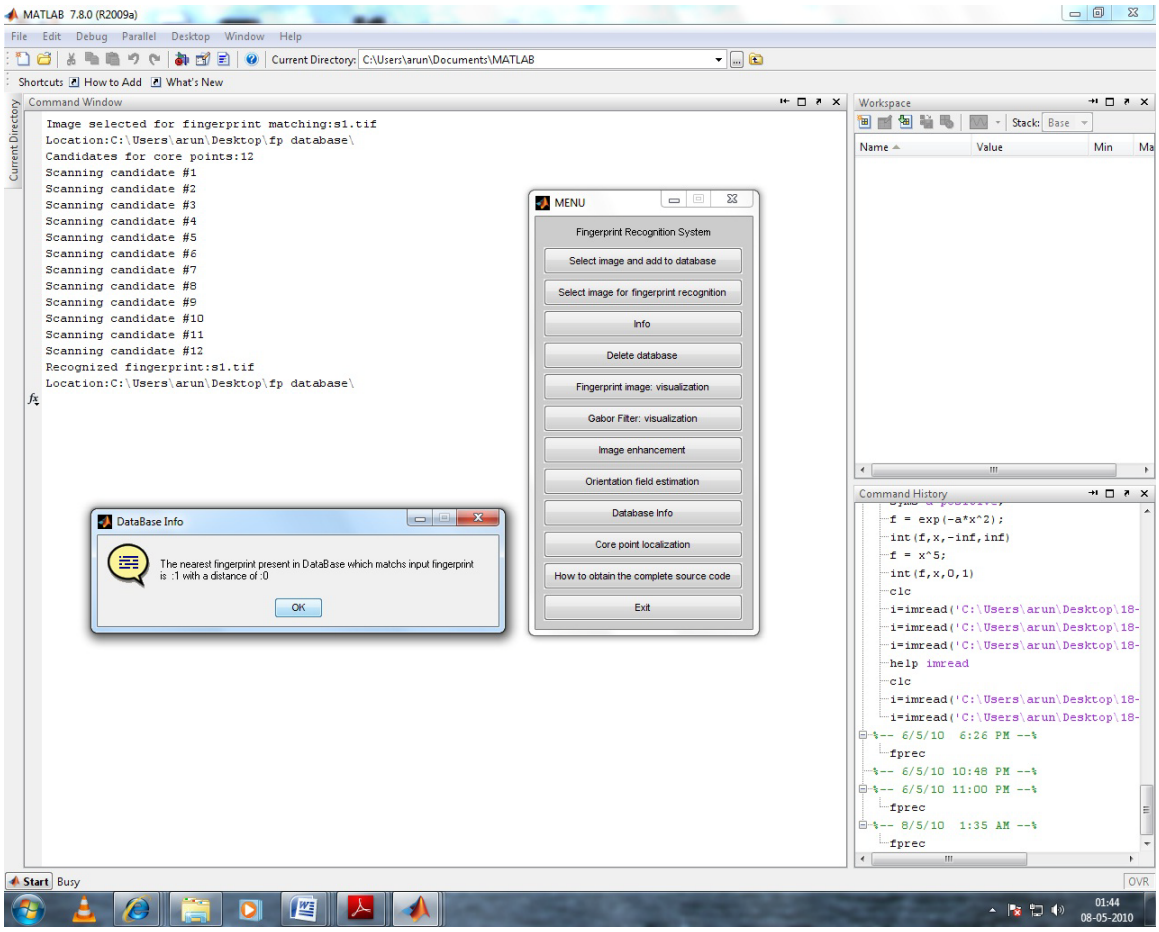


Fig 7.1.2 Sample Matlab Output (Result2)

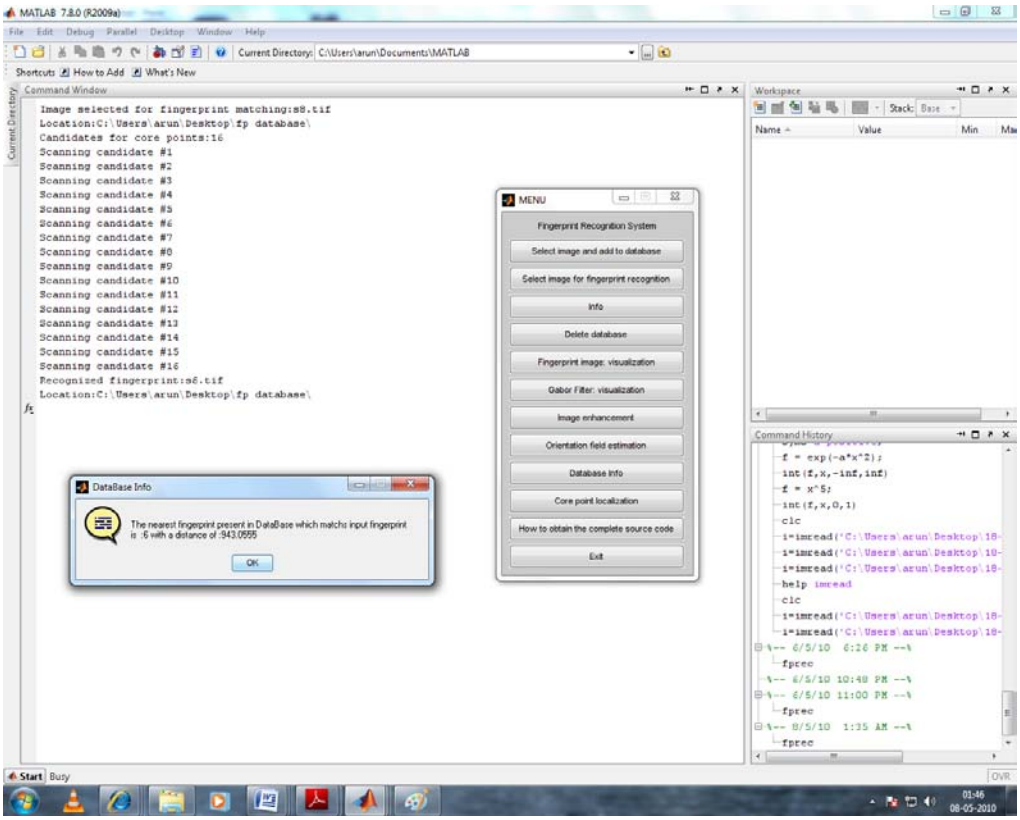
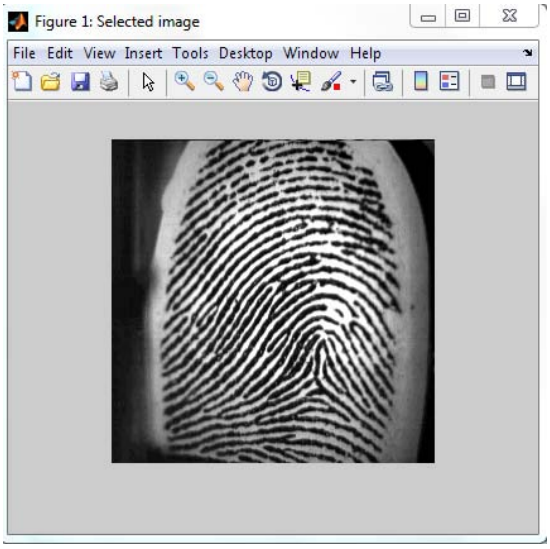


Fig 7.1.3 Sample Matlab Output (Result3)

The various processes involved in the image processing of the captured fingerprint image using the FRT are explained below.

Fingerprint image visualization

It provides us with a visual picture of the fingerprint captured and transferred from the DSP TMS320C6713 to the server computer.



Gabor filter visualization

A Gabor filter is a linear filter used in image processing for edge detection. Frequency and orientation representations of Gabor filter are similar to those of human visual system, and it has been found to be particularly appropriate for texture representation and discrimination. In the spatial domain, a 2D Gabor filter is a Gaussian kernel function modulated by a sinusoidal plane wave. The Gabor filters are self-similar - all filters can be generated from one mother wavelet by dilation and rotation.

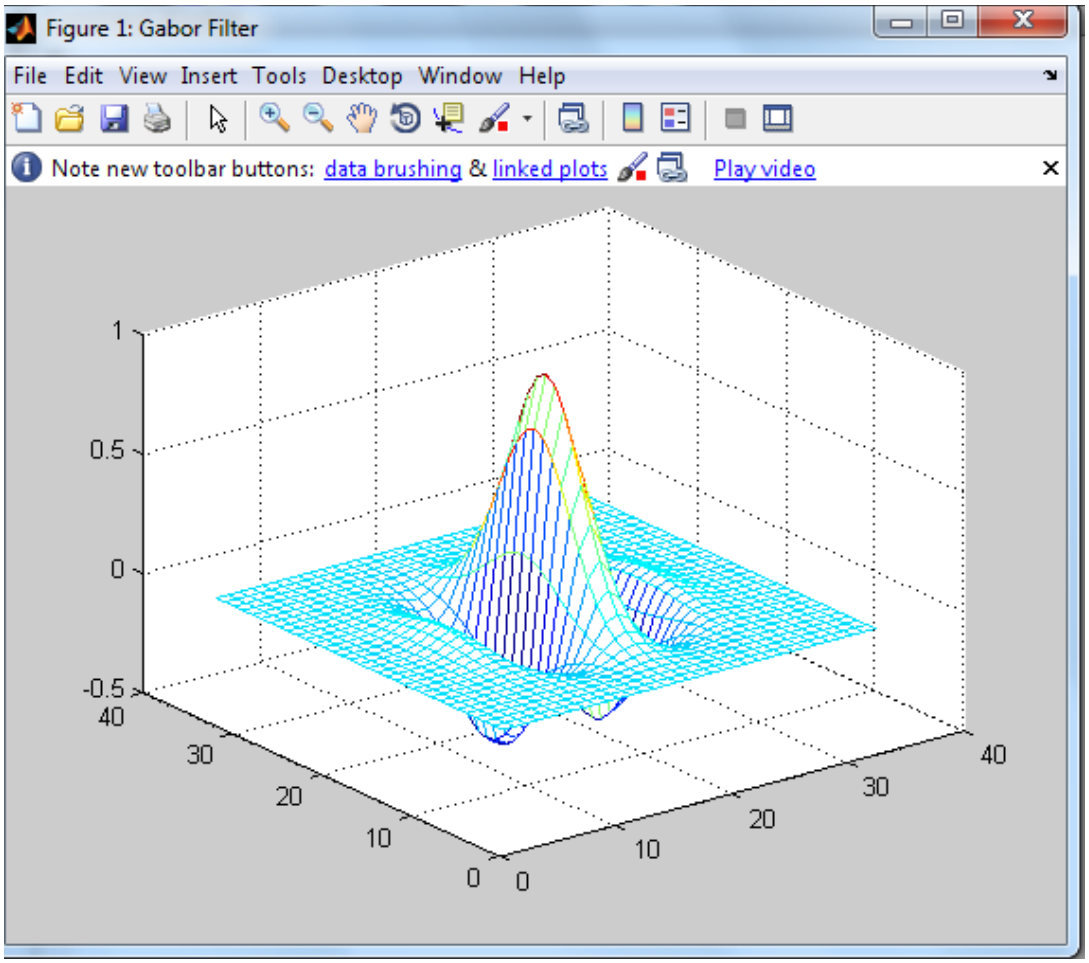
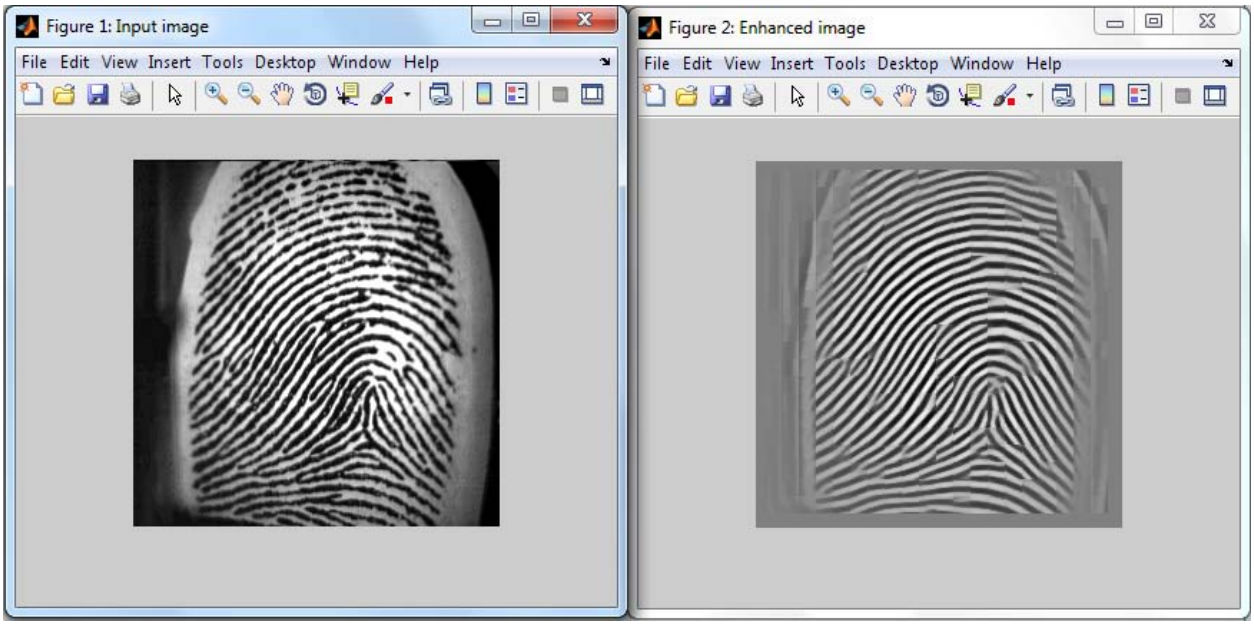


Image enhancement

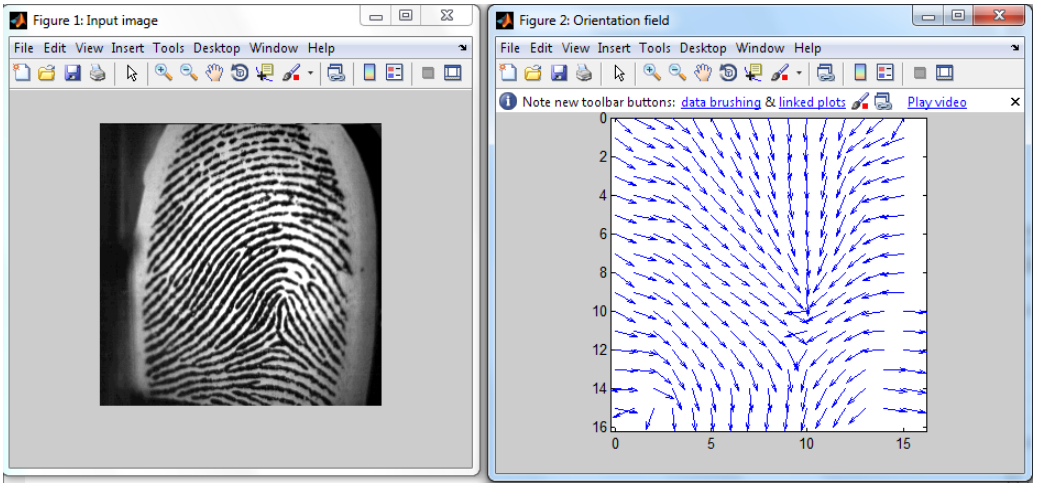
In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of input fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. It adaptively improves the clarity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency.



As shown in the above picture, the image to the right is an enhanced version of the original input fingerprint which is on the left. The input image is segmented into a matrix of cells which are individually processed.

Orientation field estimation

A directional field describes the coarse structure of a fingerprint. It describes the local orientations of the ridge and valley structures, and is useful for extraction of singular points. In general, the directional field at some location in the image is estimated by averaging the directions in a window around the desired location.



Core point localization

Core points lie in the approximate centre of the finger impression. The core point is defined as the point where convex ridges have the maximum curvature. The core-based match algorithm depends on core point to alignment the feature vector.

Chapter 8

Conclusion

8. CONCLUSION

8.1Conclusion

The fingerprints of different students were successfully enrolled and added to the database. The fingerprints were further verified and several dry runs were made that confirmed matches and mismatches for different samples. Apart from that, the FRT in MATLAB was used to demonstrate the various functions and processing methods used in image processing of the fingerprint. The outputs for all the trial runs and process demonstration were recorded.

The data transfer was made across a wireless channel in the lab connecting two terminals. Wireless communication meant that the range was limited to a short span but the data transfer process was efficient enough for the successful functioning of the system.

8.2 Future work

There is a lot of scope in the field of biometrics application at the work place. The attendance system using fingerprint recognition can be of real use if certain nuances are taken into consideration. The wireless channel used was limited to a short range and hence the system could only be tested in the lab. For a greater range and more versatile application, a different channel could be considered which would ensure faster data transfer and provide better flexibility. The security aspect of transmission can be worked upon since data security in case of sensitive data transfer is highly essential.

Finally, the proposed model for each CHM and the PC server client software management system can be materialized using cost effective products offered in the market.

9. REFERENCES

[1] *Zhang Yongqiang and Liu Ji* ,The design of wireless fingerprint attendance system, Proceedings of ICCT '06, International Conference on Communication Technology, 2006.

[2] *Younhee Gil*, Access Control System with high level security using fingerprints,IEEE the 32nd Applied Imagery Pattern Recognition Workshop (AIPR ’03)

[3] Jain, A.K., Hong, L., and Bolle, R.(1997), “On-Line Fingerprint Verification,” IEEE Trans. On Pattern Anal and Machine Intell, 19(4), pp. 302-314.

[4] D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.

[5] Lee, C.J., and Wang, S.D.: Fingerprint feature extration using Gabor filters, Electron. Lett., 1999, 35, (4), pp.288-290.

[6] L. Hong, Y. Wan and A.K. Jain, "Fingerprint Image Enhancement: Algorithms and Performance Evaluation", IEEE Transactions on PAMI ,Vol. 20, No. 8, pp.777-789, August 1998.

[7] SPRA894A, *Texas Instruments*, DSP for Smart Biometric Solutions

[8] User Manual, DWA-510

[9] SPRAA23, *Texas Instruments*, FADT2 Quick Start Guide

[10] TMS320C6713 DSK Technical Reference, (506735-0001 Rev. B)

[11] FVC2002. http://bias.csr.unibo.it/fvc2002/

[12] Fingerprint Recognition System by Luigi Rosa, (http://www.mathworks.it/matlabcentral/fileexchange/4239)

[13] Shlomo Greenberg, Mayer Aladjem, Daniel Kogan and Itshak Dimitrov, Fingerprint Image Enhancement using Filtering Techniques

APPENDIX

APPENDIX

List of some pseudo codes studied and developed for software implementation of various functions.

Pseudo code 1: Enhancement of Image

```
function [fImage]=im_enhance(InImage,f)
Im = 255-double(image);
[a,b] = size(Im);
// Apply floor function to round values of a & b; say to a1,b1
In = zeros(a1,b1);
// for 32 bit pixel data
for i=1:32:a1
for j=1:32:b1
// calculate convolution based Fast Fourier Transform
Fim=fft2( Im(i:m,j:n) );
factor=abs(Fim).^f;
// find inverse DFT of F vector multiplied with factor
Imdata= abs(ifft2(Fim.*factor));
// Normalise the obtained Imdata by dividing each element with the max. Value
In(i:m,j:n) = normalized_Imdata;
// Obtain Histogram Equalisation of image
Fimage=In*255;
Fimage=histeq(Fimage); // improves contrast of image by transforming intensity image
```

Pseudo code 2: Binarization of Image

```
function [out] = im_bin_at(im,W);
//Image is segmented and adaptive threshold is calculated
// Initialize size matrix [a,b] & output matrix out
// With step length W, divide it into blocks
//for loop for i -> 0 to a & j -> 0 to b, find mean threshold
m_thres = 0;
if i+W-1 <= a & j+W-1 <= b
m_thres = mean2(im(i:i+W-1,j:j+W-1));
m_thres = 0.8*m_thres;
//calculate output matrix using m_thres as the threshold
//scale data to colomap defined in case of 2 input arguments
imagesc(out);
colormap(gray);
```

Pseudo code 3 : Estimation of block direction

```
function [d,z] = bl_dir(Im,blsize)
// image Im is obtained from the binarization function with defined blocksize
// initialize size [a,b]& direction matrix ‘direction’, gradient matrices
W = blsize;
theta = 0;
sum = 1;
bg_present = 0;
bl_Index = zeros(ceil(a/W),ceil(b/W));
// find out the filter gradient using sobel filter
filter_grad = fspecial('sobel');
// for  x-gradient
I_x = filter2(filter_grad,Im);
%for y-gradient
filter_grad = transpose(filter_grad);
I_y = filter2(filter_grad,Im);
(loop)
// update gradient matrices and obtain the sum, subtract and no. of times value
if sum ~= 0 & times ~=0
bg_present = (times *times + minus *minus)/(W*W*sum);
if bg_present > 0.05
blockIndex(ceil(i/W),ceil(j/W)) = 1;
// Obtain value for theta from inverse tan operation on subtract & times value as limits
```

```
// find center of the image by using rounded values in x & y dir and angle value ‘theta’
center = [center;[round(i + (W-1)/2),round(j + (W-1)/2),theta]];
(end)
//scale the direction image & transform from polar to Cartesian coordinates along with velocity vectors
imagesc(direction);
[u,v] = pol2cart(center(:,3),n); // n= 16 or user defined
quiver(center(:,2),center(:,1),u,v,);
// obtain z from morphological operations and b from perimeter pixels of z.
```